

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 15843.1-2017

**Information technology -- Security techniques -- Entity
authentication -- Part 1: General**

信息技术 安全技术 实体鉴别 第 1 部分：总则

(English Translation)

Issued on: December 29, 2017

Implemented on: July 1, 2018

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the PRC**

Table of Contents

Foreword	3
Introduction	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Symbols and abbreviated terms	12
5 Authentication model	14
6 General requirements and constraints	14
Annex A (Informative) Use of text field	16
Annex B (Informative) Time variant parameters	17
Annex C (Informative) Certificates	20
Bibliography	21

1 Scope

This Part of GB/T 15843 specifies an authentication model and general requirements and constraints for entity authentication mechanisms. These mechanisms are used to corroborate that an entity is the one that is claimed.

An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities and, exchanges with a trusted third party.

The details of the mechanisms and the contents of the authentication exchanges are beyond the content of this Part and are specified in other parts of GB/T 15843.

2 Normative references

There are no normative references for this Part.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

Asymmetric cryptographic technique

Cryptographic technique that uses two related transformations: a public transformation

(defined by the public key) and a private transformation (defined by the private key).

Note: Given the public transformation, it is computationally infeasible to derive the private transformation.

3.2

Asymmetric encryption system

System based on asymmetric cryptographic techniques whose public operation is used for encryption and whose private operation is used for decryption.